at&t

Voice and Data Recovery

Emergency Coordinators Meeting, Office of Information Security and Privacy Protection

April 15, 2009

AT&T Disaster Response Process

The condition of AT&T's global network is continually monitored in our Global Network Operations Center (GNOC).

When an anomaly occurs that threatens or actually impacts the performance of our network, the response is managed by the GNOC staff through a practiced and proven incident command process called 3CP (Command, Control, and Communications).

THE AT&T GLOBAL NETWORK OPERATIONS CENTER
The world's networking company

Network Disaster Recovery

NDR Technology Trailers

- Can replace functionality of AT&T Network Node within 72 hours, not weeks or months
- Over 150 specially-designed tractor-trailers & support vehicles, housing equipment & components, self- contained or dedicated power and environmental systems
- $300M investment to provide restoration of service at AT&T sites following catastrophic event

NDR Operations Team

NDR exercises are conducted several times each year. These exercises are part of AT&T's comprehensive business continuity plan to ensure communications can be restored quickly to its government, business and consumer clients if a disaster damages or destroys parts of its network.

NDR Video

“Are You Ready?” AT&T 3 min video on Disaster Recovery is posted under “videos” on the OISPP site: http://www.oispp.ca.gov/government/default.asp

AT&T Asset Protection

Asset Protection (also known as Corporate Security) has the primary responsibility for coordinating all company efforts pertaining to the protection of company personnel, property and other assets from assault, theft, fraud, malicious damage or other criminal acts.

ALERT: COPPER CABLE THEFT

To combat copper and cable thefts, Asset Protection has dedicated a wealth of resources to public awareness campaigns and partnerships with law enforcement agencies to step up patrols of our work locations.

We’re also working with salvage yards to help them identify possible suspects and we’re encouraging them to report copper cable theft by offering large rewards for tips that lead to arrests.

Additionally, we’re working with local government and community leaders to increase criminal penalties for copper theft and those who profit from it.

To Report Copper Cable Theft Call: (800) 807-4205

AT&T and California

130 years of keeping Californians connected

- The state’s largest fiber optic network totaling 31,000+ miles
- Connect more than 300M calls a day in CA
- AT&T invested $8.3B+ in California’s economy*
- AT&T employed 46,550+ people living in California**
- Invested $2B+ in our CA networks (wireline & wireless broadband)*
- AT&T California paid/remitted $1.27B+ in local & state taxes*
- AT&T spent $1.59B+ on goods/ services to support our business in CA*
- AT&T Foundation contributed $32.6M+ to hundreds of charitable orgs. across California*

AT&T California at-a-glance

investing in California

Nationally, AT&T has a larger union workforce than the U.S. steel, auto or airline industries.

AT&T Investment in California – 2007

employment

AT&T has nearly 250 company-owned retail stores in California where our retail sales consultants help customers connect everywhere they live and work.

keeping people connected in the wake of natural disasters

*2007 Statistic **2008 Statistic

AT&T and California

130 years of keeping Californians connected

- Recently announced a $1.6M partnership with California State University
  - Aimed at increasing access to college for students in traditionally underserved communities
- Rolling out 43 alternative-fuel vehicles in 14 California cities
- AT&T responded with the largest reconstructive effort in our 130 years due to wildfires*
  - People of AT&T mobilized 1,100 technicians to support service
  - Provided 2,000 AT&T GoPhone®s and 5,000 calling cards to residents ordered to evacuate
  - Donated $150,000 to Southern California chapters of the American Red Cross
  - AT&T crews worked around the clock, replacing 500,000+ feet of fiber optic cable, 1.5M feet of copper and 2,000 telephone poles

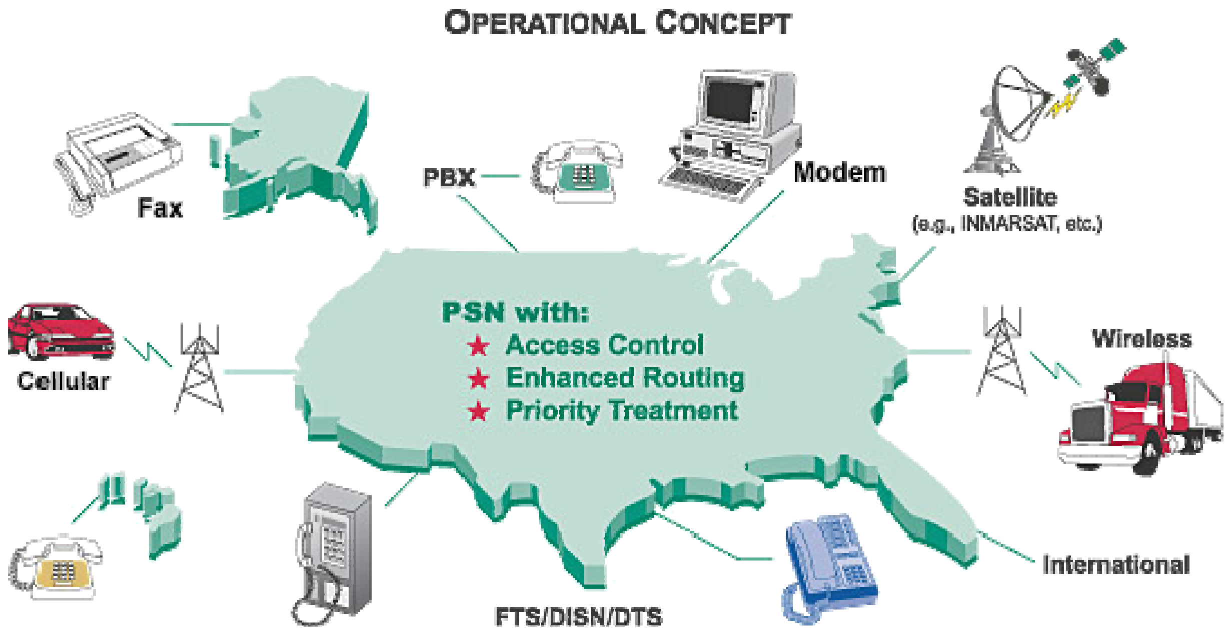
***2007 Statistic   **2008 Statistic**

Overcoming Network Congestion in an Emergency

National Communication System (NCS)

NATIONAL COMMUNICATIONS SYSTEM

Mission Statement: to provide **Priority Telecommunications Services** and other related programs to support national security and emergency preparedness efforts across Federal, State, and local organizations.



NS/EP National Security Emergency Preparedness Programs:

What are National Security Emergency Preparedness (NS/EP) telecommunication services?

NS/EP telecommunication services are services used to maintain a state of readiness or to respond to and manage any event or crisis that causes or could cause injury or harm to the population or damage to or loss of property

Telecommunications Service Priority (TSP) - a telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service.

Government Emergency Telecommunications Service (GETS) - provides emergency access and priority processing in the local and long distance segments of the public switched wireline network.

Wireless Priority Service (WPS) - provides priority cellular network access.

What is TSP?

As a result of hurricanes, floods, earthquakes, and other natural or man-made disasters, telecommunications service vendors may become overwhelmed with requests for new telecommunications services and requirements to restore existing telecommunications services.

The TSP Program provides service vendors (AT&T) with a Federal Communications Commission (FCC) mandate for prioritizing service requests by identifying those services critical to NS/EP.

Types of service requests:

1. TSP Restoral
2. TSP Provisioning

A telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service.

Non-Federal users (e.g., State, local, foreign governments) require a **sponsor**.

Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS)

Who is Authorized to Use GETS and WPS

Organizations that support one or more of the following five National Security / Emergency Preparedness (NS/EP) mission areas, qualify for NCS sponsorship to become a GETS/WPS user:

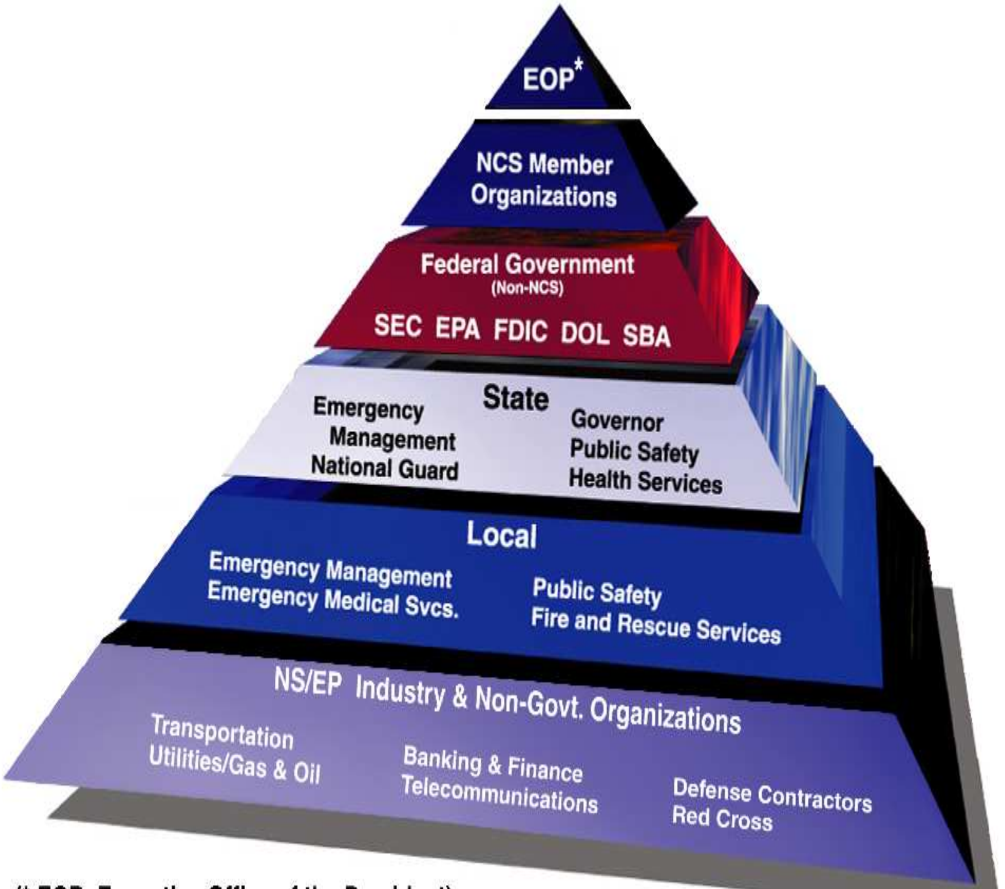
✓National Security Leadership

✓National Security Posture and US Population Attack Warning

✓Public Health, Safety, and Maintenance of Law and Order

✓Public Welfare and Maintenance of National Economic Posture

✓Disaster Recovery



EOP*

NCS Member Organizations

Federal Government (Non-NCS)

SEC EPA FDIC DOL SBA

State

Emergency Management National Guard

Governor Public Safety Health Services

Local

Emergency Management Emergency Medical Svcs.

Public Safety Fire and Rescue Services

NS/EP Industry & Non-Govt. Organizations

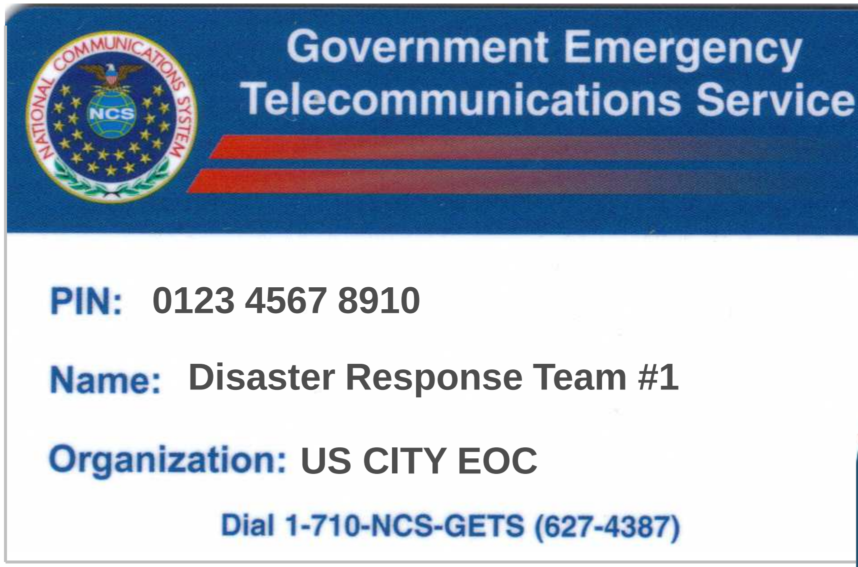
Transportation Utilities/Gas & Oil

Banking & Finance Telecommunications

Defense Contractors Red Cross

(* EOP: Executive Office of the President)

Government Emergency Telecommunications Service (GETS)



NATIONAL COMMUNICATIONS SYSTEM
NCS

Government Emergency
Telecommunications Service

PIN: 0123 4567 8910

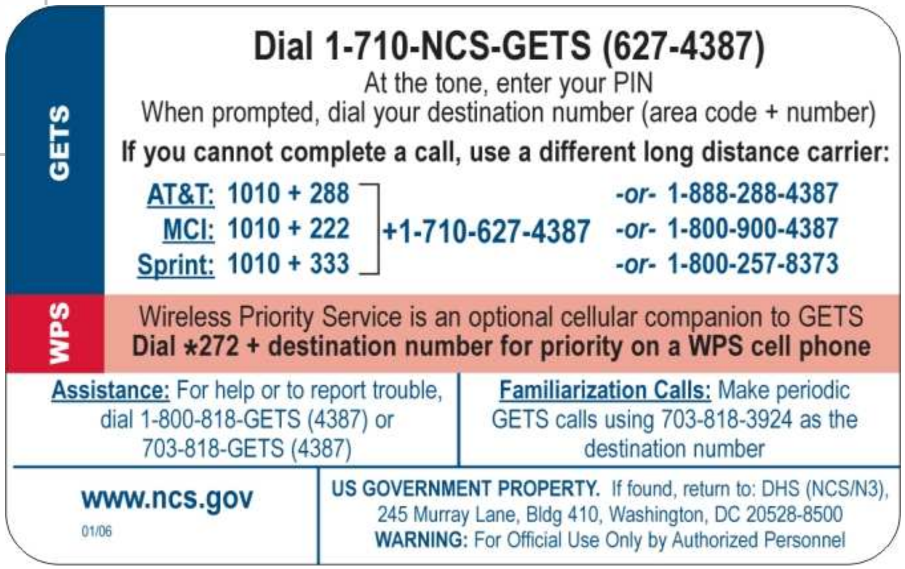
Name: Disaster Response Team #1

Organization: US CITY EOC

Dial 1-710-NCS-GETS (627-4387)

GETS priority is invoked
“call-by-call”

GETS is a "ubiquitous" service in the Public Switched Telephone Network…if you can get a DIAL TONE, you can make a GETS call



GETS

Dial 1-710-NCS-GETS (627-4387)

At the tone, enter your PIN

When prompted, dial your destination number (area code + number)

If you cannot complete a call, use a different long distance carrier:

AT&T:	1010 + 288	+1-710-627-4387	-or- 1-888-288-4387
MCI:	1010 + 222		-or- 1-800-900-4387
Sprint:	1010 + 333		-or- 1-800-257-8373

WPS

Wireless Priority Service is an optional cellular companion to GETS
Dial *272 + destination number for priority on a WPS cell phone

Assistance: For help or to report trouble, dial 1-800-818-GETS (4387) or 703-818-GETS (4387)

Familiarization Calls: Make periodic GETS calls using 703-818-3924 as the destination number

www.ncs.gov
01/06

US GOVERNMENT PROPERTY. If found, return to: DHS (NCS/N3), 245 Murray Lane, Bldg 410, Washington, DC 20528-8500
WARNING: For Official Use Only by Authorized Personnel

Wireless Priority Service (WPS)

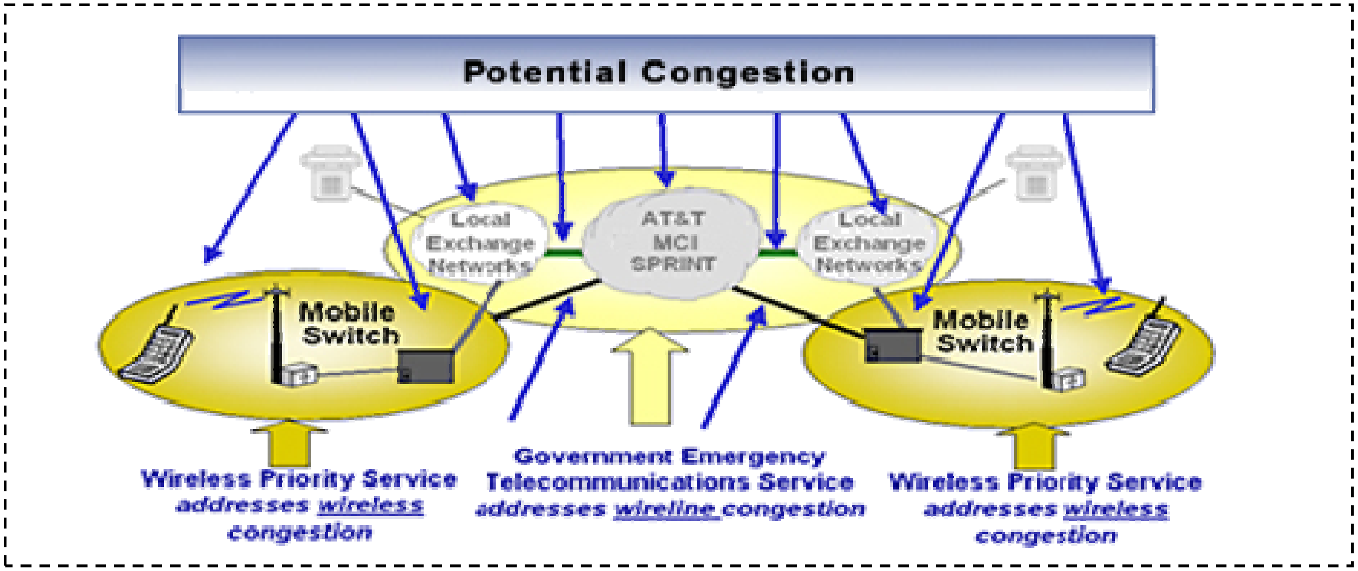
- A powerful but under-utilized feature for public safety!
- Provides agencies like fire, police, Dept. of Justice, Homeland Security, the Department of Defense, and others priority access in heavy network traffic.
  - Available in all AT&T Mobility home GSM coverage areas
  - Managed by Federal GETS (Gov. Emergency Telecommunications Service)
- How it works
  - Register your SIM card/phone number with the WPS (http://wps.ncs.gov)
  - Users are assigned a priority rating (1-5 based on organization type and requestor role)
  - Once WPS is activated, just dial *272 plus your destination number
  - Your call will be flagged as an urgent communication and the next available radio resource at the cell level will connect you

What offers the most coverage?

A powerful but under-utilized feature for public safety!

Provides agencies like fire, police, EMS, Health Services, and others priority access in heavy network traffic.

If landline networks are also congested, utilize *272 **plus** the GETS access number to get priority in both wireless and landline networks.


Potential Congestion
Local Exchange Networks
AT&T MCI SPRINT
Local Exchange Networks
Mobile Switch
Mobile Switch
Wireless Priority Service addresses wireless congestion
Government Emergency Telecommunications Service addresses wireline congestion
Wireless Priority Service addresses wireless congestion

NCS Helpful Tips

- Many organizations have an established Point of Contact (POC) for administering GETS and WPS.
- If you are part of a Federal, state, local, tribal, or industry organization and are unsure if there is an existing POC, please complete the **Need to know if your organization already has a POC** form located at: **www.wps.ncs.gov**
- The Priority Telecommunications Service Center will contact you within five business days.
- For assistance and information on all NCS Priority Telecommunications programs contact the Priority Telecommunications Service Center toll free at 866-627-2255 (DC metro area, please use 703-760-2255) or gwids@saic.com
- Main site: **www.ncs.gov**

National Coordinating Center

Receive an aggregated report that reflects the availability of all communications assets in the affected area 703-235-5080.

The NCC leverages its unique joint **government/industry** structure and all-hazard **emergency response capabilities** to coordinate the initiation, restoration, and reconstitution of United States government national security and emergency preparedness telecommunications services both **nationally and internationally.**
National Coordinating Center for Telecommunications

Safe Accountability for Every Port Act of 2006

Warning Alert Response Network (WARN)

WARN ACT

Warning Alert Response Network

October 2006

The WARN Act will create within the Department of Homeland Security, a voluntary **National Alert System** to provide a public communications system capable of alerting the public on a national, regional, or local basis to emergency situations requiring a public response.

The National Alert System will:

- ❑ enable any Federal, State, tribal, or local government official with credentials …. to alert the public to any imminent threat that presents a significant risk of injury or death to the public
- ❑ be coordinated with and supplement existing Federal, State, tribal, and local emergency warning and alert systems
- ❑ transmit alerts across the greatest possible variety of communications technologies, including digital and analog broadcasts, cable and satellite television, satellite and terrestrial radio, wireless communications, wireline communications, and the Internet to reach the largest portion of the affected population

http://www.fcc.gov/pshs/cmsaac/

WARN Advisory Committee Preliminary Findings:

- Mass notification technology uses consumer email text messaging gateways to send alert notification messages.
- The consumer email gateway is unsuitable for bulk or urgent notifications. Its only intended use is personal, individual, non-critical person-to-person communications, and it is explicitly unsupported for any bulk application-generated messaging.
- The messaging gateway is also subject to tens of millions of SPAM messages each day. Because of the ease in guessing email addresses, this service is actually subject to more SPAM than the typical ISP. Bulk and broadcast messages behave nearly identically to SPAM messages and could be blocked by the SPAM control systems in the network.
- Text messaging capacity limitations prevent it from being employed as an emergency broadcast solution. While sufficient capacity exists at local levels for normal messaging delivery, broadcast messages cause congestion in the network, which may result in delayed delivery of messages or blocking of text messages and voice traffic.

SMS Notification Key Problem: "Stack Up" In Emergencies

One example of how quickly SMS can stack up in an emergency:

Sample: Washington, DC

- Assume that the city has an average density of 8,388 people/sq mi
- Assume the city is covered by 40 cell sites with 120 sectors
- Assume an average sector covers approximately 6000 people and has an approximate capacity of 120 messages per minute
- If 60% of the city's population sent a text message at the same time, or 3600 subscribers send 3600 messages per minute in each sector…..

Result: **the system generates 3600 messages/minute in each sector, or *30 times greater* than the 120 SMS/min a sector can process**

Source: "SMS over SS7," National Communications System - Technical Information Bulletin 03-2, December 2003

Best Practices For Wireless Notification Systems

- Prioritized messaging to mobile subscribers is key (send messages to key government/first responders *first*
- Before selecting a notification system vendor, ensure they have tested for interoperability with all providers
- Messaging to wireless subscribers should be a small part of your overall notification plan
  - ❑ Use other/additional delivery methods such as home/dorm phone, work phone, email, Blackberry/PDA/Pager, radios, TTY/TTD, public broadcast systems, indoor/outdoor warning systems and digital signage, word-of-mouth/door-to-door
  - ❑ Consider carefully when directing people to contact other phone numbers, web sites, ect. for additional information

at&t

Best Practices for State Government

Emerging Technologies

Dynamic Acceleration with Increased Interactions

Initiatives

Telepresence / Collaboration Tools

Disaster Recovery – Enterprise Backup Planning

Cloud / Utility Computing / SAAS

Viral/Malicious or Productivity Reducing Activity Protection

Hosted VOIP & Call Center

Asset Tracking – RFID / GPS

ER Apps

311

Gov e-commerce

Jail Video Visitation

Tele-medicine

Mobility Resource Management – X- force automation

Business Intelligence (BI)

Highly Available

24 x 7 x 365

Interactions

Security

Mobility

Hosting

Enhanced Communication

Virtualization

Business Continuity

Enablement

Network Based

Managed Solution

Customizable

Legislative Drivers for Business Continuity Solutions

Ruling	Who Is Impacted	Regulatory Challenges
SEC 17a-4 | 17a-3	Broker/ Dealers	*Email, Instant Messaging must be stored for 3 yrs, in 2 separate & distinct places, & must be easily accessible*
NASD 3010	Broker/ Dealers	*Requires 'supervision' including implementation a formalized review process of incoming/outgoing emails & instant messaging*
Federal Reserve/ SEC/OCC	Financial Institution	*Specific Business Resumption Recommendations* ▪ **Resume business within 2 hrs.** ▪ **Recover financial transactions within next business day** ▪ **Ensure Back-Up Facilities are "Out Of Region" from Primary Site** ▪ **Perform cross organization tests to assure compatibility**
Sarbanes-Oxley	CEO, CFO, Public Firms	*A broad auditing, financial disclosure & corporate governance law.* *Imposes substantive rules as to the conduct of a publicly-held company*
HIPAA	Healthcare Insurance	*Standardize the use & transfer of oral, printed, & electronic records.* *Privacy & Security driven (protects the disclosure of all patient health information)*
Financial Services Modernization Act (Gramm-Leach-Bliley)	Financial	*Requires banks to develop privacy notices & give their customers the option to prohibit banks from sharing customer information*
FDA - Title 21 CFR Part 11	Pharmaceutical	*Outlines criteria for acceptance by the FDA of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper*
Basel II	Financial	*Relates to where and how a financial institution's information and data is provided and controlled*
California SB 1386	Any Entity Dealing w/ CA Residents	*Businesses must inform residents if their name, SS#, Driver's license, Credit Card, or Bank account were compromised*

Risk Assessment and BC Planning-

9 Questions About Your Business Continuity Plan

Mitigate Risk, Protect Mission Critical Data

1. Have you analyzed which business processes, applications and services are most critical?
2. Have you assessed the impact of a potential disruption?
3. Have you created a strategy to mitigate risk?
4. What security measures are in place?
5. Are key locations hardened, conditioned facilities?

Meet Customer and Regulatory Requirements

6. Have your customers or business partners mandated performance or availability service levels?
7. What current or emerging regulatory requirements must be complied with?

Invest Wisely

8. Have you quantified the potential costs of downtime or total business failure?
9. Have you developed sound business cases to optimally invest in risk mitigation?

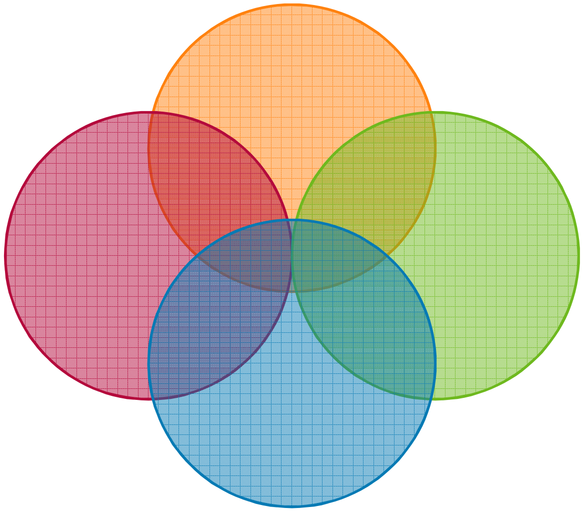
AT&T Business Continuity Capabilities

	Prevention & Mitigation	Response & Recovery
People	• Corp BC Planning • Remote VPN Access • LaptopConnect • Crisis Phone Program	• Network Disaster Recovery • Wireless Voice: Wireless Priority Service, Video Share • Wireless Data: Laptop Connect, Enterprise Paging, email • Corporate Crisis Management • Audio- and Web-conferencing • Contact Center Services
Processes	• Corp BC Planning • BC Professional Services	• eTools: EOD and Premier • StorageConnect^{SM} recovery service • BusinessDirect® eMaintenance & Ordering
Network and Infrastructure	• Corp BC Planning • Network Disaster Recovery • Wireless WAN Connectivity Back-Up • Commercial Connectivity Services • Ultravailable® Network • Hosting & Application Management • StorageConnect^{SM} - Managed Data Storage Services • Security Services and Secure Email Gateway	• Network Disaster Recovery • Wireless WAN Connectivity – Temporary Primary • Enterprise Recovery Service • Enterprise Messaging hosting infrastructure • BusinessDirect® performance monitoring and call routing • eTools: Coverage Viewer

AT&T Business Continuity Services

Professional Services

- ➢ Business Continuity Professional Services



Wireless Solutions

- ➢ Video Share
- ➢ Connectivity Services
- ➢ LaptopConnect
- ➢ Wireless Priority Services
- ➢ Crisis Phone Program
- ➢ Email Portfolio
- ➢ Enterprise Paging

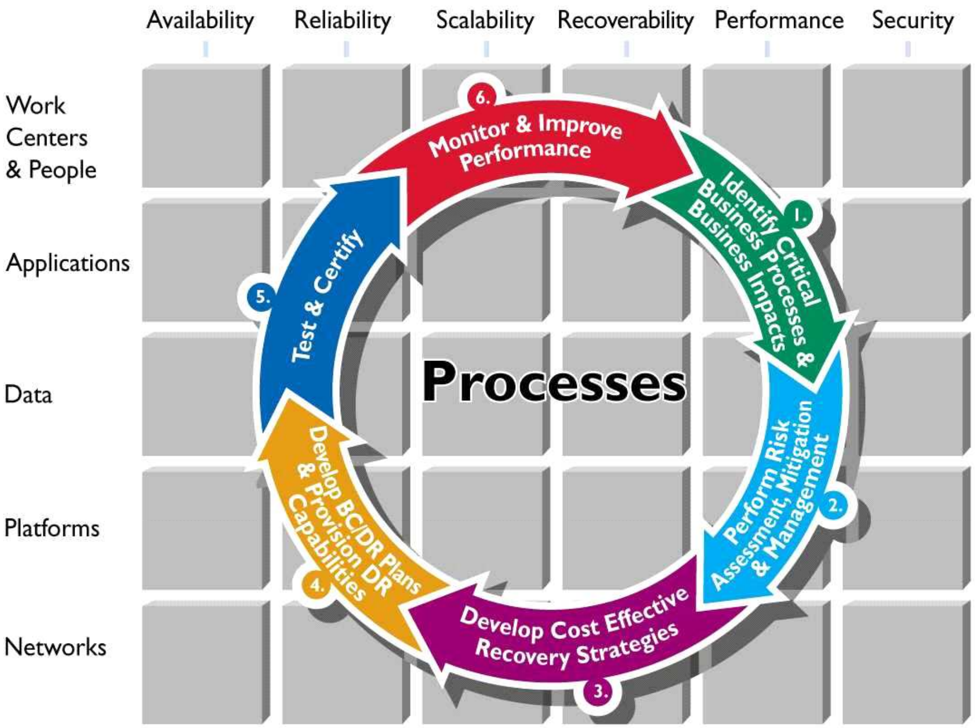
Network Services

- ➢ Ultravailable® Network Services
- ➢ StorageConnect^{SM} Services

Data Protection and Recovery Services

- ➢ Enterprise Recovery Services
- ➢ Tape and Disk Backup in IDCs
- ➢ Storage Services in IDCs
- ➢ Remote Vault^{SM}

AT&T Business Continuity Professional



Availability
Reliability
Scalability
Recoverability
Performance
Security
Work Centers & People
Applications
Data
Platforms
Networks
Processes
1. Identify Critical Business Processes & Business Impacts
2. Perform Risk Assessment, Mitigation & Management
3. Develop Cost Effective Recovery Strategies
4. Develop BC/DR Plans & Provision DR Capabilities
5. Test & Certify
6. Monitor & Improve Performance

Practices

Managed Risk Services

- Business Impact Analysis
- Risk Assessment
  - Mitigation Strategy Development

BC Strategy and Planning

- BC Strategy Development
- BC Plan Development
- BC Plan Testing
- BC Plan Certification
- Emergency Response Planning
- Emergency Response Testing

BC Program Management

- BC Standards Development
- BC Program Metrics
- BC Program Review

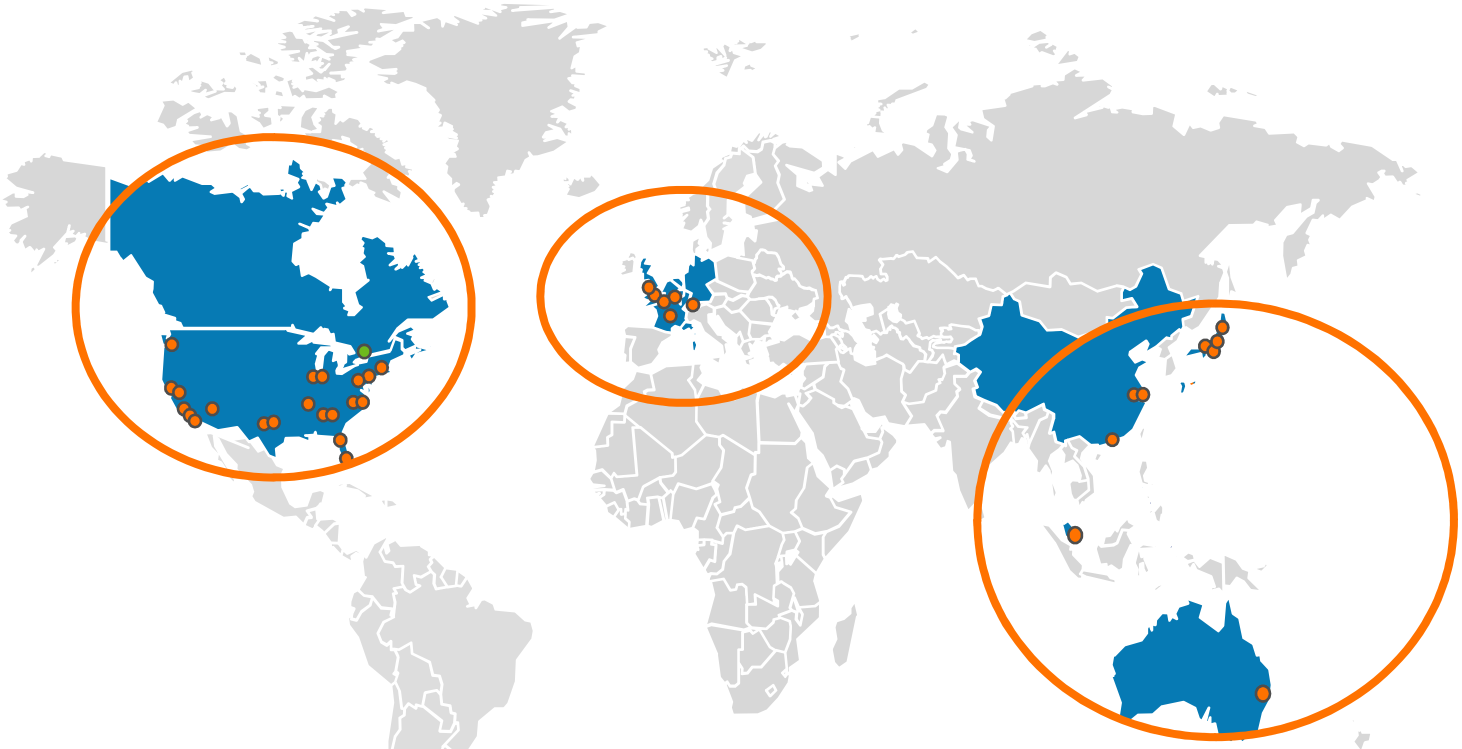
Features

- Examination of operations, critical processes and services with tailored solutions
- Design, deployment and management of business continuity solutions to meet business processes and supporting infrastructure
- Certified Business Continuity Professionals
- Methods to mitigate the financial and operational impacts of business disruption

Benefits

- Identify and quantify their present state of readiness
- Develop strategies to keep business resources up 24x7
- Mitigate financial and operational impacts of business disruption
- Identify risk exposures and strategies to mitigate risk
- Ensure continuous business operations
- Free up valuable resources to focus on business operations

38 AT&T Internet Data Centers Worldwide



North America - 23

Annapolis, US
Atlanta Area, US (2)
Boston Area, US
Chicago Area, US (2)
Dallas Area, US (2)
Los Angeles Area, US (2)
Miami, US
Nashville, US
New York, US
New York Metro Area, US (2)
Orlando Area, US
Phoenix Area, US
San Diego Area, US
San Francisco Area, US
San Jose Area, US
Seattle Area, US
Toronto, Canada
Washington DC Area, US

Europe - 6

Amsterdam, NL
Birmingham, UK
Frankfurt, DEU
London, UK
Nice, FR
Paris, FR

Asia Pacific - 9

Hong Kong, CH
Osaka, JP
Shanghai CH(2)
Singapore, SG
Sydney, AU
Tokyo, JP (3)

at&t

Wireless Continuity of Government

Dave Pearce, Mobility Application Consultant

Continuity of Government/Disaster Recovery Mobility Challenges

- Enable critical personnel to communicate in emergencies
- Provide “interoperable” mission-critical communications across groups and organizations
- Provide key staff with emergency alerts and access to vital data
- Provide critical team members with mobile voice and data access in emergency situation
- Keep devices on hand in “voluntary suspend” mode, ready to be activated when a crisis or emergency arises
- Enable fixed offices and remote workers to stay connected in disaster/crisis situations

Wireless Communications

Diversity by Nature

- **Survivability**
  - Multiple Cell sites eliminates single point of failure
- **Mobile Flexibility**
  - Service is not location specific – move to areas of coverage
  - Multiple modes: IM, eMail, voice messaging and data applications
- **Fast Recovery**
  - Wireless facilities can be established almost anywhere
  - COW – Cell on Wheels; Mobile cell sites can be driven into a disaster area

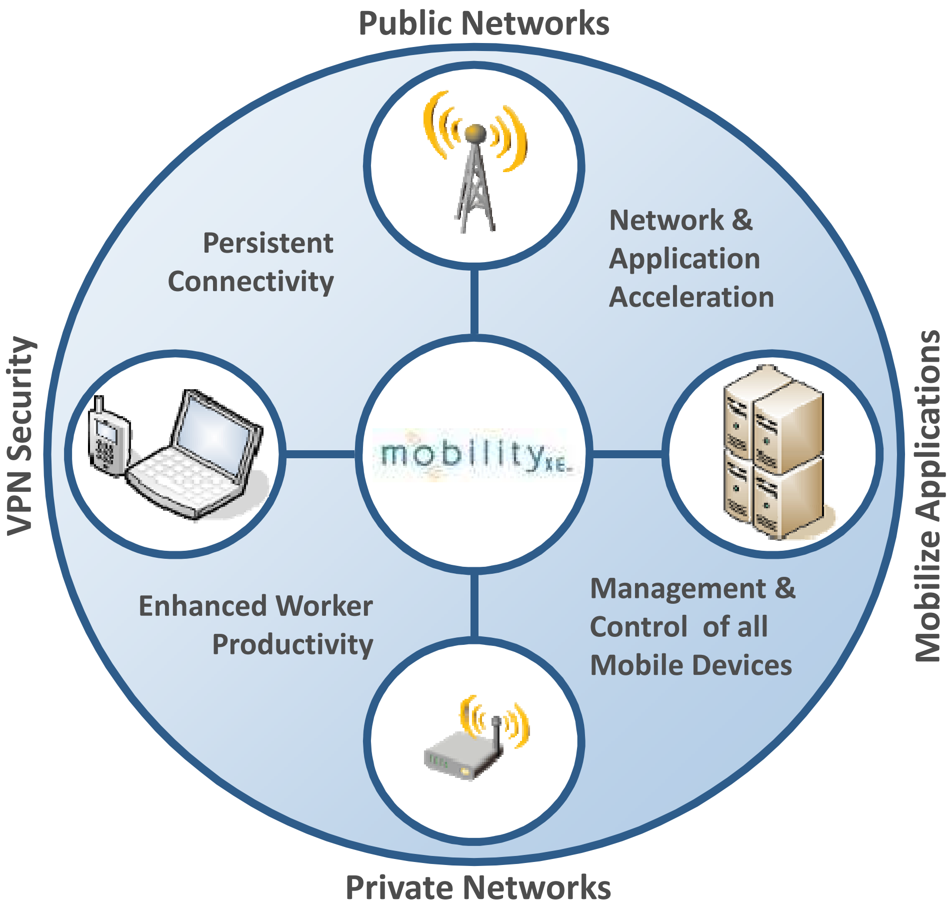
AT&T Continuity of Government/Disaster Recovery Mobility Solutions

- Customer-deployable emergency cellular base stations
  - AT&T product: satellite-based GSM connectivity from **AT&T Mobility Vanguard**
  - GSM base stations (large or small) connected to AT&T public network via satellite backhaul link
  - Designed and being used today on board cruise ships and other maritime applications
  - Can be easily adapted for on-land whitespace coverage or emergency/COOP deployments!
- Interoperable field communications between radio, cellular and IP networks
  - Available from AT&T: **Codespear SmartMSG**
  - Wireless data & video distribution
  - Secure audio and data recording & logging
  - Support for cellular, satellite, Wi-Fi & private networks

AT&T Continuity of Government/Disaster Recovery Mobility Solutions

- Emergency mobile device supplies
  - AT&T product: **Crisis Phone/Voluntary Suspend** program
  - Devices are purchased at regular price and suspended with a recurring charge of $.01 per month.
  - If a device needs to be activated, contact your AT&T representative
  - When a device needs to be activated, it will bill at the contracted monthly and usage rates, until re-suspended
- Mobile connectivity as a backup to wireline connections
  - AT&T product: **WWAN Backup**
  - Uses 3G aircard + router as an emergency backup to any DSL, private line or other IP circuit

Mobile Optimized VPN Solution: NetMotion Mobility XE


Public Networks
Persistent Connectivity
Network & Application Acceleration
VPN Security
mobilityXE
Mobilize Applications
Enhanced Worker Productivity
Management & Control of all Mobile Devices
Private Networks

VPN built for mobile, wireless

Client/Server software

- Supports all current Windows OSes

Low cost installation & maintenance

- Deploy in under an hour

Security

- Control application access by user, device, etc.
- RADIUS, AD/NTLMv2, SecurID authentication
- FIPS 140-2 validated AES 128-256b encryption

Productivity

- Eliminates disconnects, shut-downs, sign-on, etc.
- Seamless roaming & accelerated throughput
- Real-time access to more applications

Management

- Centralized web-based management console
- View device connection details
- Low effort to support large mobile deployments

NETMOTION WIRELESS

Solutions Brief: Secure Wireless Email

Forwarding agency email to a wireless handheld device provides a secure mobility extension of an office PC. In addition to all email functions, contacts, and calendar functions are synchronized, and meeting invitations can be created or responded to. Many wireless email applications are FIPS 140-2 certified, and some have additional security like s/MIME and CAC Reader support. Compatible with Microsoft, Lotus, and Novell email platforms.

Problem / Challenge

- Device security concerns have limited agency's use of PDA's for personal information management
- Security policies from NIST and DISA have prevented adoption of remote wireless access to LAN
- Concerns of variable cost have limited deployments to only select few within agency.

Wireless Enablement

- FIPS140-2 certified application with device security and remote security meet NIST security requirements
- Wireless implementation limited to email servers only; policies established for permissible/prohibited email use
- Selection of AT&T's multiple email plans and devices allows for cost-effective deployment to multiple levels

Post-Wireless Result

- Increased productivity across the board; users are able to make down time productive time
- Decision drag reduced significantly – anytime, anywhere decision-making enabled.
- FISMA Information Security guidelines met

Deployments

United States Senate

US Postal Service

US Air Force

US Marine Corp

Internal Revenue Service

NIST
National Institute of Standards and Technology

FIPS VALIDATED 140-2

DEVICES

Smartphone Security Management

TRUST DIGITAL™

Trust Digital is a leading provider of enterprise smartphone security and management software, securing smartphones that have access to corporate information. By implementing Trust Digital's policy-based solution, corporations eliminate the risks associated with accidental or malicious disclosure of data.

NETWORK

AT&T has the largest voice and data network in the United States; Service plans are available to government agencies under Networx, GSA and various other purchasing vehicles

at&t

Solutions Brief: Secure Wireless Remote Access

Wirelessly-enabled laptops and middleware can provide NIST-compliant secure remote access to sensitive, but unclassified agency networks while maintaining persistent connectivity between 802.11x WiFi and AT&T's nationwide data networks. Security policy management tools provides additional capabilities to insure agency-unique policies are enforced. Compression utility optimizes user experience in sub-optimal conditions

Problem / Challenge

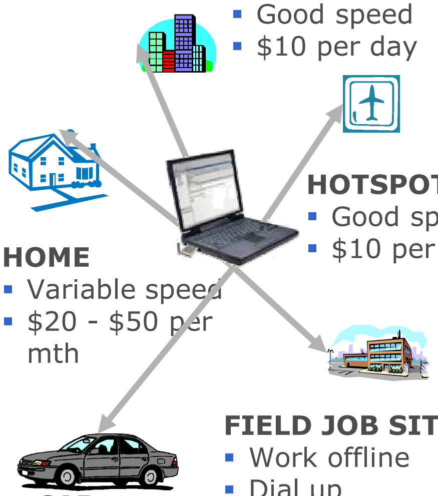
- Concerns that public networks are not secure
- Don't want employees accessing network in public hotspots even if WPA-2 encrypted
- Need connectivity where WiFi access is not provided

Wireless Enablement

- Dedicate servers for wireless remote access to network
- Deploy laptops with WiFi and AT&T Data capability, either embedded or with Type II PC or CF Card
- Install Netmotion Mobility XE VPN client & Server software
- Provision AT&T's unlimited, nationwide data plans
- Set up and implement Security Policy Manager

Post-Wireless Result

- Simplified security platform for both WiFi and AT&T data networks
- Users can move in and out of WiFi, 2G and 3G data coverage without having to re-establish connection to network each time.
- Users happy with remote access experience



HOTELS

- Good speed
- $10 per day

HOTSPOTS

- Good speed
- $10 per use

HOME

- Variable speed
- $20 - $50 per mth

FIELD JOB SITE

- Work offline
- Dial up

CAR

- Work offline
- Dial up from pay phone

Replace traditional expenses with Unlimited Data for $59/mo

DEVICE

Type II or CF Cards

Embedded Laptops

Encryption-Persistence-Compression

NETMOTION WIRELESS

Mobility XE provides the highest form of AES encryption at 256 bit; Mobility XE middleware also provides compression, session persistence and device policy management.

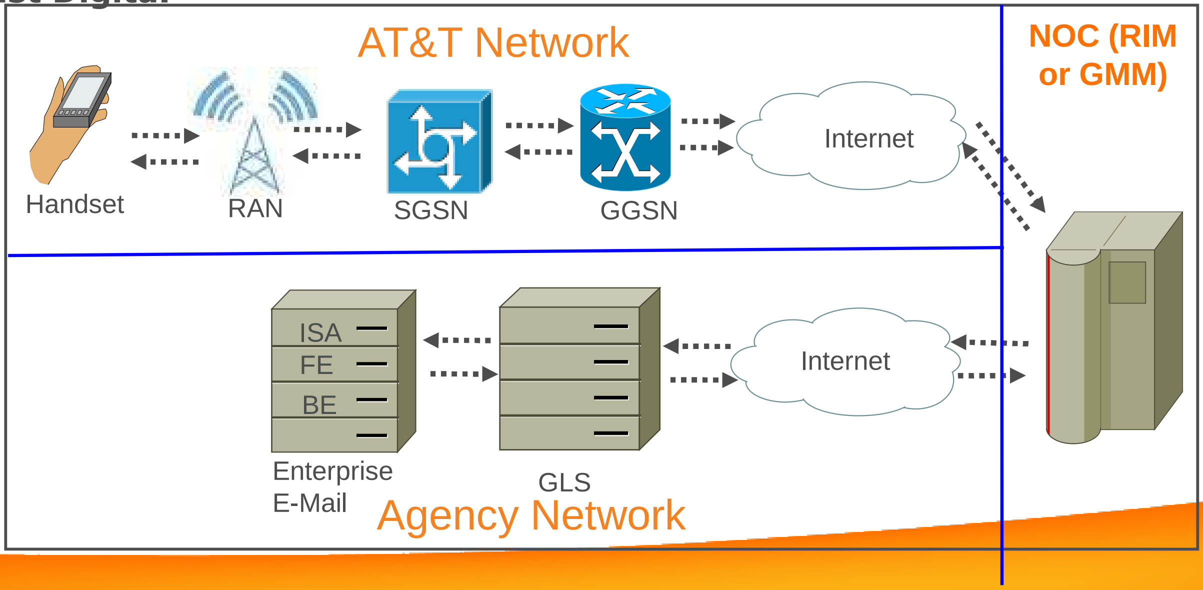
NETWORK

AT&T has the largest voice and data network in the United States; Service plans are available to government agencies under Networx, GSA and various other purchasing vehicles

at&t

Secure Push E-mail/Mobile Device Management Systems For SBU Applications

- Major commercial enterprise mobility systems provide options for e-mail/data security in transit and at rest
  - NOC-based messaging systems
    - Provides a bridge between the enterprise e-mail system and a Network Operations Center (NOC)
    - AT&T supports **BlackBerry** and **Good** – both have S/MIME CALs that allow NIPRnet access
  - Direct push messaging systems
    - Provides a bridge directly from the e-mail system to the mobile device
    - **Microsoft's Direct Push** (MSDP) – requires third-party device management system such as **Trust Digital**



Commercial Connectivity Service (CCS)

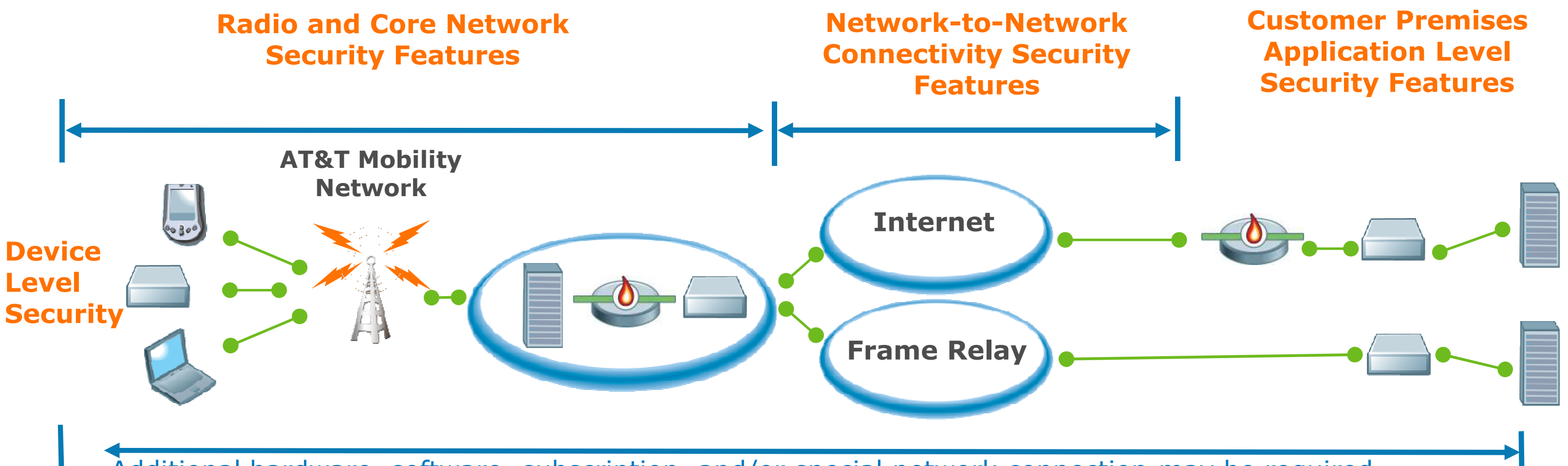
End-to-end security enhancements for Wireless Network Connectivity

Standards based connectivity

- Secure connectivity from AT&T to customer premise
  - Frame Relay or Internet (IP) Secure Channel
- Network enabled airlink encryption (128 bit on 3G/ 64 bit EDGE)
- Traffic segregation with custom Access Point Name (APN)

Options plus Geo Redundancy

- Customizable IP addressing - Public/Private and Static/Dynamic
- Firewall/access control and Mobility data center redundancy
- Variety of Frame Relay and Internet connectivity solutions
- Multiple provider connectivity
- Traffic can be shifted to unaffected locations during disaster scenarios


Radio and Core Network Security Features
Network-to-Network Connectivity Security Features
Customer Premises Application Level Security Features
AT&T Mobility Network
Device Level Security
Internet
Frame Relay

Additional hardware, software, subscription, and/or special network connection may be required.

AT&T Local Resources

Pat Newquist, Sr. Account Manager, pn3989@att.com

Mark Roese, Technical Sales Manager, mr5713@att.com

Thank you

Beth Kerrick

Industry Solutions Practice Manager,

bethk@att.com

Dave Pearce, Mobility Applications Consultant